softchoice

SECURITY & STORAGE

ADVISOR

TECHNOLOGY BUYING GUIDE

What's Inside

- Protect Yourself from Cybercrime
- What's New in Data Backup
- Continuous Data Protection
- Network Access Control 101

WINTER 2007

1.888.SOFTCHOICE | WWW.SOFTCHOICE.COM/ADVISOR

Local. Accountable. Personal.
That's the Softchoice difference.

Working with you face to face is our way of acknowledging that technology challenges aren't managed by technology, but by thoughtful, dedicated people. People who provide deep insights and who take your best interests to heart.

At Softchoice, face-to-face service is our most important value we add. Why? Because getting to know you in person means a better understanding of your business needs, better advice, and better IT solutions. It's an approach that's personal and powerful. It's also our way of ensuring that every IT investment you make delivers results.

With a local presence in more than 34 cities across North America, chances are we're already a part of your community. Give us a call and experience the difference – up close and in person.

softchoice

Answering Your Technology Needs

softchoice

SECURITY & STORAGE

ADVISOR

TECHNOLOGY BUYING GUIDE

IN THIS ISSUE:

04 Introduction
Finding your way to IT enlightenment.

06 Data Backup Protection
Two trends have combined to bring big changes to backup technology.

12 Continuous Data Protection
Continuous Data Protection is leaving other storage solutions in the dust.

16 Network Access Control
No network is airtight - malware continues to get in.

18 Data Security
Shields Up Mr. CIO. (Just make sure they are encrypted).

See What Face to Face Can Do for You

Smart People, Smart IT Decisions

Your local Softchoice representative will help you navigate the wide range of volume discount programs to identify a purchasing strategy that makes sense for you and your bottom line.

Your Industry Go-to.

Get answers you can trust. Our dedicated team of product specialists is your point of contact for product demos, detailed information on purchasing options, and easy access to the manufacturers themselves.

Great Selection. Great Delivery

Representing more than 4,000 leading hardware and software manufacturers, chances are we've got what you need. Plus we back it up with next-day delivery to virtually any city in North America.

Optimize Your IT Investments.

IT asset management is more than just counting PCs. Our TechCheck assessment services can help you gain actionable insights into your IT environment to help you drive efficiency, reduce risks, and manage technology more effectively.

Click.
www.softchoice.com

Call.
1.888.SOFTCHOICE

In Person.
Contact a Softchoice Representative.

Bringing the Best in the Industry Right to Your Door

brother · EQUALLOGIC · hp invent · IBM Business Partner · KASPERSKY lab · lenovo · McAfee · Quantum · SOPHOS · symantec · TREND MICRO

Want to be added to our mailing list?
Visit www.softchoice.com/advisor

Want to be removed from our mailing list?
Visit www.softchoice.com/unsubscribe

The Softchoice Advisor is the recipient of the CEA 2006 Gold Award for Best Channel Marketing Initiative

The Softchoice Advisor publication comes to you free from Softchoice Corporation. Corporate Softchoice headquarters is located at 173 Dufferin Street, Suite 200, Toronto, Ontario, Canada M6K 3H7. Information and pricing are subject to change without notice. Errors and omissions excepted. All manufacturer names are registered trademarks of their respective corporations. No part of this publication may be reproduced by any means without written permission. © 2007 Softchoice Corporation. Concept and execution by Softchoice Marketing Department. Printed in Canada. ISSN 1715-8672 **Softchoice Advisor VOLUME 3 - EDITION 7**

Security and Storage – Finding Your Way to IT Enlightenment

Avoiding all the security and storage pitfalls can be hard. Whether it's fending off pesky viruses, preventing identity theft, or planning ahead in the event of a disaster, these days IT managers have a maze of issues to navigate. One wrong turn, and your organization could find itself increasing its risk, wasting time, or draining valuable IT resources. That's why Softchoice wants to help guide you to the best security and storage solutions in the business.

Backup & Email Archiving

Is your email server near capacity? Do you have a small timeframe for backing up your data? Perhaps it's time you contacted a Softchoice's Vendor Sales Specialists (VSS). A VSS can provide expert purchasing and technical advice on behalf of major storage partners such as EqualLogic, EMC, Lefthand, Quantum, and many others. Available anytime, they're your point of contact for product demos, detailed information on purchasing options, and easy access to the manufacturers themselves. We've got your backup covered.

Compliance

Regulatory bodies like Sarbanes-Oxley and HIPAA have mandated that organizations have the ability to retrieve old records in a reasonable amount of time. That means finding the right storage solution. Softchoice can make your search easier by leveraging the appropriate resources and expertise. Whether it's accessing our own in-house technical sales specialist, connecting you to a local service partner, or one of our vendors, Softchoice can help get you the right advice, and the right solution to your storage needs.

Disaster Recovery

As the reliance on business-critical data continues to rise, so does the need for disaster recovery solutions. Through our leasing and financing services, Softchoice can put an effective disaster recovery solution well within reach. Our cost-effective leasing options are designed to reduce your total cost of ownership, keep you current, and streamline your technology acquisition processes. There's no time like the present to plan ahead.

Email Spam

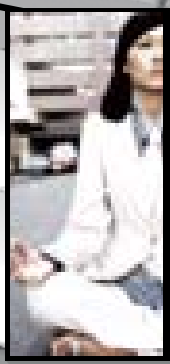
Avoiding annoying SPAM mail is critical for the smooth operation of your business. Eliminating SPAM means keeping your employees on task, eliminating inappropriate content, and securing your network from threats. Trust Softchoice to help you select the right solution for SPAM mail, or any other security-related issue. With our selection of over 30,000 security products, we give you real choice you can count on!

Identity Theft

Preventing phishing scams, weak passwords, and malicious intruders from compromising your IT environment means having access to the right people, and the right technology. At Softchoice, we're happy to meet with you in person to get to know your business, your challenges and create a plan to help you optimize every IT investment you make. And you can forget about automated phone trees. When you call Softchoice you're guaranteed a live, knowledgeable, response every time.

Virus, Spyware & Attacks

Roughly 49% of all business PCs contain moderate to severe spyware infestations, while one in every 16 is likely missing anti-virus software altogether. Good thing Softchoice's assessment services make it easy and cost-effective to maintain a secure IT environment. By leveraging data from any type of IT management solution, we can help you identify the gaps between corporate policy and infrastructure reality as well as spot missing patches, service packs, and anti-virus software. The best part? You can dramatically reduce your security risks with almost no time or resources invested on your part. Now that's peace of mind!



IT Enlightenment

Getting your IT environment to the right place can be quite a journey. You need the best tools and resources to manage risk, secure data, and protect your corporate reputation. Softchoice can help by offering enterprise-wide solutions that address your unique challenges and reduce the cost and complexity of managing technology. Now that's a worthy destination.

the state of Data Backup Protection

By Howard Marks
Network Computing

For most of the past 20 years, making backups has involved a potentially incendiary combination of tedium and little opportunity for reward, plus high career risk if things go south. The only variation to this routine occurs when vendors try to get us excited with new versions of the same backup software or bigger, faster tape drives. Year after year we back up from disk to tape, and when it comes time to restore, we search for the right tapes. Whoopee.

But now, two trends have combined to bring big changes to backup technology. Vastly decreased costs for both disk drives and bandwidth make it worthwhile to reconsider your backup setup. It might be a pain in the neck, but maturing technologies, such as VTLs (Virtual Tape Libraries), and increasingly intelligent backup software have "evolutionized" corporate backup.

The first trend is the free fall in the cost of high-capacity ATA and SATA disk drives and arrays. Keeping a gigabyte of data on disk once cost 10 times as much as storing the same data near-line in a tape library. Since disk costs have fallen faster than tape costs, the difference in now less than 5-to-1.

Not only are SATA drives much less expensive than the Fibre Channel and SCSI drives used to host high-performance applications, the sequential nature of writing backups to disk plays to their strengths. High-performance drives have intelligent-command queuing, shorter settle times and higher rotation speeds that accelerate the kind of random I/O a database performs. But the capacity-optimized SATA drives can handle sequential I/O just as well as their pricier cousins.

The second change is that as quickly as disk space costs have fallen, so have bandwidth costs. The industry frenzy to lay more and more fiber across the world in the 1990s created a bandwidth glut that's made multi-megabit connections affordable even for residential use.

The challenge we face as system managers is to figure out which technologies, like backup to disk, are really sea changes, and which ones, like server-less backup across the SAN, will turn out to be a great idea on paper but a bust in real life.

The most obvious impact of falling disk prices has been the rapid adoption of disk-to-disk backup. Most system managers change from tape to disk as their primary backup medium to speed up their backups. Unless they're still using DLT8000 drives, they soon discover that the speed of the tape drives isn't the limiting factor in how fast most of their backups run.

Backing up to disk lets you back up more data in the same amount of time not so much by accepting data faster, but by letting more backups run in parallel. Unless it's multiplexing, which has its own problems, a backup application can send only one stream of data to a tape drive at a time. Because tape drives in libraries are expensive, the number of drives available limits the number of backups most organizations can run in parallel.

Modern tape drives have a voracious appetite for data. They move tape at 120 inches per second and ingest data at up to 120 MBps. If a backup stream can't keep the drive fed, it must stop the tape, rewind past the point where it left off and start recording again. Not only does this increase the wear and tear on the tape drive, it also slows down the process significantly.

Backing up to disk addresses both these problems. A disk array has no inherent limit on the number of backup streams it can handle and will accept data as fast as the media server can deliver within the limits of the connective fabric. Clever backup admins can

schedule a lot of slow backups, like the dreaded Exchange brick-level process, to a single disk target simultaneously.

Although disk is cheap, nothing can beat the cost of tape on the shelf, which can run as little as 10 cents per gigabyte. Experience tells us that frequency of restore requests falls off rapidly over time, so most organizations spool stale backup data from secondary disk to tape for longer retention. Tape also has the advantage of portability, so organizations that don't replicate data to a disaster-recovery site or use an online backup service, can ship their data offsite for disaster recovery.

Aside from vendor pitches and hype, for most organizations the tapeless data center makes as much sense as the paperless bathroom.

Although faster backups may be the sizzle, faster and more reliable restores are the steak of disk-to-disk backup. It's now a given that while we may back up in preparation for a full-server restore, most restore requests are for a few files that a user "lost" in the past 30 days. Even if the tape with the data is still in the library, mounting the tape and fast forwarding to the desired file takes a few minutes. If the tape must be found and mounted, turnaround time can stretch to days. Because even disks emulating tapes in a VTL are random-access devices, there are no mount and fast-forward delays. Files can be restored in seconds instead of minutes.

> "...for most organizations the tapeless data center makes as much sense as the paperless bathroom."

What's the best way to use tape for backup? Backup apps take differing approaches. Some, including Symantec NetBackup and Tivoli Storage Manager, can use disk purely as a cache. The data is temporarily stored to disk until a given backup job is completed, then it's spooled to tape. Others, such as Atempo's Time Navigator and BakBone's NetVault, turn one or more disk volumes into a VTL with a predefined number of tape drives and cartridge slots. Usually the program just writes to a disk, which creates a backup file for one or more backup jobs. Then each backup file is treated like a tape cartridge.

Backup To Disk Appliances

Ever since Quantum announced its DX-30 VTL in 2003, overworked system administrators have latched onto VTLs as the easy way to integrate disk into their existing backup plans. All they have to do is change the destination for some of their backup jobs to the new VTL. Because the VTL connects to the SAN like a real tape drive and mimics a real tape library, no other disks are needed.

Regardless of how well a VTL does its job, though, it's still emulating a tape library and subject to the limitations of that technology. Once a tape is written it can be appended, but the data on the tape can't be modified or deleted. If a virtual tape contains some successful backups and the data from one or more failed backup jobs, the backup administrator can't delete the data from the failed jobs without overwriting the whole set.

A few years ago we would have said that VTLs are great for overburdened admins, but not for long-term use. As applications added their own backup to disk functions, we expected administrators to redesign their backup processes to save on the added cost of a VTL. We predicted they'd take advantage of the greater flexibility in media management that treating disk as disk provides.

If a backup app really understood disk storage, it could delete files at the end of their retention period; let administrators delete the data from temporary, failed or partial backups; and show the amount of available space on the target. Unfortunately, that kind of flexibility is still a pipe dream. None of these tasks are easy with current tools, nor are they possible with tapes--virtual or not.

But the VTL vendors have made progress. The most significant is data de-duplication. With data de-duping, the VTL identifies files, and portions of files, that have been backed up before. Instead of saving an additional copy of that data, it uses a pointer to the previous copy. End users running data de-duping devices report that they can store 10 or 20 times as much data on their backup appliances than the disk capacity of the VTL would suggest. Even with the additional cost of a VTL over raw disk de-duplication, it makes disk backup less expensive than tape in the library.

The list of vendors that now offer this de-duping feature is long. It includes Diligent's ProtecTIER, Quantum's DXi series, Sepaton's Deltastor and FalconStor's latest version of its VTL software. This software is OEM'd by vendors including EMC in its Clariion Disk Library.

The other addition VTLs have made is replication. Once data is de-duplicated, backup appliances from FalconStor and Quantum can replicate the new data across an IP network to another remote backup appliance. For applications that don't require short RPOs (Recovery Point Objectives) this is a cheap way to get data offsite.

Finally, recognizing the media-management advantages of a file-based solution, vendors including Data Domain and Quantum provide a NAS interface to their backup appliances as well as tape library emulation.

Synthetic Backups Go Down Market

Organizations using the typical weekly full backup and nightly incremental process have to manage two backup windows. Nowadays many organizations must retain data for longer periods to comply with SOX and HIPAA. Other companies just don't bother to delete old data. As a result, time for incremental backups may remain the same as that allotted for full backups. To solve this problem, specialized backup applications like EMC's Retrospect and Tivoli Storage Manager only make a full backup the first time they protect a server or file system. From that point on, backups are incremental. When a backup administrator wants to restore a file, the application finds the most recent version. If an admin needs to send a full backup offsite for disaster recovery or archiving, the application copies the latest versions of each file from all the backups of the server. It then builds a synthetic full backup set. ○

Copyright © 2007 CMP Media LLC.

Read the full article at
www.softchoice.com/marks

A Brilliantly Simple Way to Control Who Gets In

Sophos NAC Advanced – simple to install, simple to use

Sophos's tough, effective, yet remarkably easy-to-deploy solution works with your existing infrastructure to ensure everyone accessing your network conforms to your security policies. It's that simple.

Endpoint Security & Control with NAC Advanced, 100 – 199 users –12 months

$55.50 USD / $66.50 CAD

SKU: V32312 / V32313

SOPHOS

Quantum GoVault Data Protection Solution

An Ideal Disk-based Data Protection Solution for Small Business

GoVault Data Protection Solution is the ideal backup product for SMB customers looking to upgrade their current backup devices with an easy-to-use, affordable disk-based solution.

Fast - Backup completes BEFORE you leave the office

Simple - Limited backup management resources required

Reliable - Worry-free protection with archive shelf life of 10+ years

Affordable - Advanced protection within existing budget

Solution - Includes dock, cartridges (onsite/offsite) and data protection software (featuring data de-duplication technology)

Quantum

CUSTOMER SERVICE:

We're in IT to help you

Technology doesn't solve problems, people do. That's just one of the reasons a Softchoice representative will be happy to meet with you in person to understand your goals and create a plan to help you optimize every IT investment you make. And you can forget about automated phone trees. When you call Softchoice you're guaranteed a live, knowledgeable response every time. Experience the difference. Call us today.

softchoice

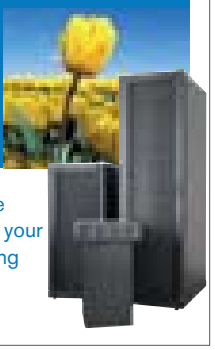
EQUALLOGIC®
SIMPLIFYING NETWORKED STORAGE™

BECAUSE YOUR STORAGE IS SUPPOSED TO BE SCALABLE

MEET YOUR GROWING STORAGE DEMANDS

Adding storage for your Microsoft® servers should be completely hassle-free – whenever you need it. The PS Series from EqualLogic transparently expands to match your growth needs and ensure data availability for all your Microsoft servers, including Exchange, SQL, and Web content management.

The PS Series offers unmatched performance to match your needs today – with room to grow tomorrow.



Find out what scalable storage from EqualLogic can mean for your Microsoft environment by calling 1.888.SOFTCHOICE.

Reliable, Manageable Performance

HP StorageWorks D2D110 Backup System

The HP StorageWorks D2D110 Backup System provides reliable, consolidated data protection for up to four servers in a single, self-managing device. It works with your backup software application to fully automate daily backup jobs, requiring less manual handling – a real benefit for organizations with limited IT resources. The HP D2D Backup System also increases the reliability of your backups by reducing the risk of human error in managing tape drive and media hardware, the two major causes of failed backups. This disk-to-disk backup solution lets you easily restore lost or corrupted files from online backups within minutes.

The HP StorageWorks D2D110 Backup System gets users back to work quickly, reducing downtime costs and frustration while contributing to the overall productivity of your business.

NAS · 1 TB · HD 250 GB x 4 · Gigabit Ethernet · iSCSI · Smart Buy

$1,701 USD* / $2,031 CAD*
*price subject to change

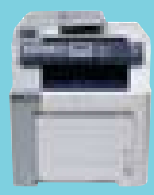
US/CAN SKU: T63674

hp invent

Break new ground in business,

convert

to colour laser.



$869.99
MFC-9440CN

Our **MFC-9440CN**'s user-friendliness and reliability means you finish printing, scanning, copying and faxing more quickly for your business.

Network
• Network-ready, with built-in Ethernet interface[1].

Print
• Up to 2400 x 600 dpi colour laser output, at up to 21 ppm*. USB drive and PictBridge compatible.

Scan
• High quality colour scanning, up to 19200 dpi (interpolated).

Copy
• Crisp colour laser copying with multi-copy and sorting functions.

Fax
• 33.6 Kbps high speed super G3 faxing and PC Fax.

START
INVEST in your business at brother.ca/smb
NETWORK

*Up to 21 pages per minute in colour and monochrome. [1]Cables not included. Price may vary. Brother and its logo are trademarks of Brother Industries Ltd., Japan. All specifications are subject to change without notice. All registered trademarks referenced herein are the property of their respective companies. ©2007 Brother International Corporation (Canada) Ltd. 1, rue Hôtel de Ville, Dollard-des-Ormeaux, Québec, H9B 3H6

At your side.
brother

The Rise of Cybercrime

How to Protect the New Mobile Workplace

Today's technologies offer business people countless ways to communicate and collaborate, creating a new work environment that's no longer confined by the boundaries of the corporate network. The dark underside of this newfound freedom has the potential to unleash a windfall for cybercriminals.

Organizations need to find ways to extend network protection to reach remote users and an increasingly mobile workforce. Flexibility in corporate computing is critical to protect against existing, new, and unknown security threats – such as viruses, spyware, rootkits, hacker attacks, phishing, spam, and other malicious programs.

Defend Every Node on the Network. It's becoming impossible to pin down where the network perimeter ends. Customizable and scalable protection is needed for every node – from mobile phones, laptops, and workstations to file servers, mail servers, and Internet gateways.

Protect Against All Threats. The threat of Internet attacks is increasing exponentially (80,000 new attacks in 2006 alone). The use of social engineering techniques has changed the threat landscape. Solutions need to combat all classes of cyber-threats.

Deliver Rapid Response. With today's threats going global, real-time response is a necessity. Proper defense requires rapid discovery, analysis, and distribution of countermeasures. Look for solutions that not only offer top detection rates, but also fast outbreak response times and near real-time protection updates.

Stay Ahead of the Threat. For complete protection it comes down to the right combination.

A solution with signature-based protection and advanced proactive technologies is the right choice for recognizing the warning signs of malicious activity before it happens.

Prevent Any Intrusion. Advanced heuristics are very effective at detecting password and data theft. Together with a personal firewall and an intrusion detection/prevention system, activity can be closely monitored to prevent intrusion into/out of a system.

Travel Safely. When working outside the corporate network, remote users need specially created policies that kick in as soon as they disconnect and reconnect to the network.

Kaspersky Lab is setting the new security standard for protecting today's distributed workforce from the gateway to the end points.

Company Profile

Kaspersky Lab delivers the world's most immediate protection against IT security threats, including viruses, spyware, crimeware, hackers, phishing, and spam while having the lowest system utilization impact (6%) in the industry. Kaspersky Lab products provide the world's highest detection rates*, the industry's fastest outbreak response time,** and standard automated hourly updates directly from the renowned Kaspersky Internet Security Lab. More than 200 million users are protected by the company's premium security solutions. This technology is inside more than 120 leading global IT security, networking, and messaging software companies. Learn more at www.kaspersky.com

Corporate licensees for Kaspersky Lab's complete line of award winning products are now available from Softchoice.

Call 1.888.SOFTCHOICE for more details.

*AV-Comparatives.org & AV-Test.org

**CNET

KASPERSKY lab

Stop threats early
Before they damage your network

InterScan™ Gateway Security Appliance

All-in-one security appliance that blocks viruses, spyware, spam, and other threats at the Internet gateway.

KEY BENEFITS

- Stops spam and other threats in-the-cloud and at Internet gateway
- Combats web-based malware by rating a web site's reputation and URL filtering
- Blocks access to malicious websites, preserving network resources and employee productivity
- Enables easy deployment and management, with support from TrendLabs (SM) experts
- Simplifies security for medium businesses with a single, all-in-one solution

100 users, 1 yr. maintenance
$966 USD / $1,001 CAD
SKU: S08390

Try and Buy available via
www.softchoice.com/trendmicro

TREND MICRO™

Protect *more.* Know *more.* Manage *less.*

Now available at Softchoice! The McAfee IntruShield network IPS solution

The world's only network IPS solution to receive new "multi-gigabit IPS" certification by NSS Group

When it comes to securing your network, point products aren't the most efficient or the most accurate option. For intelligent, comprehensive enterprise-level protection for every network-connected device, rely on McAfee IntruShield®. Our high-performance, award-winning network IPS appliance efficiently integrates risk and threat knowledge. The result? Real-time, actionable security.

www.softchoice.com/mcafee

McAfee®

Data storage at its finest

From the reliable HP StorageWorks family

The HP StorageWorks Ultrium 920 tape drive is the highest-capacity, fastest performance half-height tape drive in the StorageWorks family based on HP's third-generation LTO technology. The Ultrium 920 delivers a compressed storage capacity of 800 GB per data cartridge and a compressed data transfer rate of 432 GB per hour—two and a half times faster than the previous generation. The Ultrium 920 is the ideal choice for mid-range servers with enterprise-class data protection needs.

Tape drive · LTO Ultrium (400 GB / 800 GB) · Ultrium 3 · SCSI LVD · external · Smart Buy

$2,104 USD* / $2,498 CAD*
*price subject to change

US/CAN SKU: T51383

hp invent

Quicker. Faster. Better.

Continuous Data Protection is leaving other storage solutions in the dust

By Mark Sebastian
Softchoice Security and Storage Sales Manager

An organization's number one asset is its data. Whether it's an email message, an accounting spreadsheet, research data, or a customer database, information is essential for companies to operate efficiently and effectively. If your employees don't have proper access to data it can lead to loss of productivity, loss of revenue and, in some cases of prolonged outage, closure of the business.

To help protect valuable information, organizations usually employ a daily backup process and simply hope data can be recovered in the event of a disaster. Traditional backup solutions, such as using tape, are often sufficient for this. However, with the increasing amount of data that companies need to retain to comply with laws and regulations such as Sarbanes-Oxley, quicker solutions are going to be necessary. That's why continuous data protection (CDP) is rapidly becoming the best option for protecting your data.

Continuous data protection means backing up data by automatically saving a copy of every change made to that data. If you're working on a large spreadsheet, for example, every time you save the file the change is copied by the CDP solution. If someone were to delete the file after you've been working on it for, say, four hours, an administrator would be able to restore the latest version. With traditional nightly backup, however, you would have the ability to restore only the file from the day before, and that means losing the four hours of work. CDP can work with many types of data, including files, emails, databases, and logs. The saved copy of changes allows an administrator to restore data to any point in time, making it easier to restore lost or damaged data in less time than a nightly backup takes. The copying of changes usually occurs between separate storage locations, either in the same server room or at different sites.

Some backup solutions replicate data at every change, whereas "snapshot solutions" copy changes at specific intervals. CDP essentially eliminates the need for a backup window if there are no offsite storage requirements. Changes are copied automatically throughout the day as changes occur, thus making the restoration of any data from any point in time possible. This allows for quick restoration of deleted, virus-infected, or accidently over-written files. With snapshot CDP, backup windows are reduced since changes are being copied at specified intervals (e.g., once every 30 minutes). Data can then be restored at these specific times if needed.

When using a CDP solution, organizations will still need to store the data changes somewhere. In most cases the data will be stored on devices such as a DAS, NAS, or SAN. Changes can be kept indefinitely or purged at a predetermined time. This is similar to retention policies for backing up with tape. However, with CDP, a company will save large amounts of storage space since it's not wasting space with full backups.

The usefulness of a CDP solution is contingent on a company's recovery time objective (RTO). The RTO is the amount of time in which a system should be up and running after an outage or a disaster. For core systems, this is critical. Imagine your administrator informing users that the email system won't be back up for a couple hours, or even days! With CDP, you can ensure quick and up-to-the-minute recovery of data, or up-to-the-minute replication of data to a remote site. This protects your data, as well as your company's reputation.

CDP can be implemented as a hardware or software solution. Hardware-based solutions will perform the data copying and store the changes. Hardware is easier to deploy and set up and comes in an appliance form or as a SAN feature (SAN-to-SAN replication). A software solution will need to be installed on a server with agents deployed to the systems you'd like to protect. This is probably the most cost-effective solution, depending on whether a server or storage is required. However, setting it up can be complicated and you may find yourself reaching for the user manual.

Has CDP completely replaced the traditional backup to tape? It all depends on an organization's environment. If an IT manager deploys a CDP and changes are copied in the same server room or building, then the company will still need to use backup tapes to fulfill offsite storage requirements. If the CDP deployment utilizes a remote site, there won't be a need to keep as many tapes offsite since technically there will be two copies of the data.

Another factor that comes into play with backup is adherence to laws and regulations such as Sarbanes-Oxley. Your organization may need to keep your data for long periods (three to seven years) based on some of these laws. CDP data would not be used to adhere to these regulations, which is why there is still a requirement that backup tapes be used. It's important to note that although they seem similar, CDP is not considered data archiving. CDP is about copying data, whereas archiving is the process of moving data from one storage area to another.

"...although they seem similar, CDP is not considered data archiving. CDP is about copying data, whereas archiving is the process of moving data from one storage area to another."

There's another way of reaping the benefits of CDP and that's with laptop data. Significant amounts of corporate data can be found on laptops, but users usually don't create backups of their files or they store them on file sharing sites as instructed by their administrators. Other users work from home, so they have no access to file sharing or they call the helpdesk to help them recover their files. In the event of a stolen or misplaced laptop or a hard drive crash, CDP ensures that the files can be recovered. This can save a company time and recovery costs – not to mention a lot of unnecessary stress.

So is CDP right for your organization's storage needs? First, look at the type of data you need to protect and ask yourself the following questions:

- Do I need fast recovery of data?
- Is my RTO for my core systems measured in minutes and not hours or days?
- Is my backup window shrinking quickly?

If you answered yes to any of the above, then your company may be a good candidate for continuous data protection. You'll need to first decide at what intervals you'll need to copy changes, where to store the copies, and whether to go the hardware or software route. Budget, timing, and resources will definitely come into play, but if you need advice, Softchoice can help. We partner with leading hardware and software vendors that provide CDP solutions and we'll help you choose the right storage device for your unique requirements. That's storage done right! ○

Personal and Corporate Security Made Easy

ThinkVantage® Client Security Solution

Lenovo's unique hardware-software combination helps protect your company information including passwords, encryption keys and electronic credentials. Some features like fingerprint authentication for notebooks and desktops, file encryption and password management help guard against unauthorized user access to data.

Don't risk personal or company information. Three-level protection ... that's secure!

Available on most ThinkPad and ThinkCenter units.

lenovo

The Next Generation of Symantec AntiVirus
New Symantec Endpoint Protection 11.0
Symantec™ Endpoint Protection combines Symantec AntiVirus™ with advanced threat prevention to deliver an unmatched defense against malware for laptops, desktops, and servers. It delivers the most advanced technology available to protect against today's sophisticated threats and threats not seen before. It includes proactive technologies that automatically analyze application behaviors and network communications to detect and actively block threats. It also provides device and application control features to manage actions and secure data. Symantec Endpoint Protection seamlessly integrates these essential security capabilities in a single agent that is administered via a single management console to reduce the costs, complexity, and administrative overhead associated with managing multiple endpoint security products.
symantec™

Achieve 55% Lower Costs for Virtualized Environments

Introducing the IBM System Storage™ N3300, the newest addition to IBM's enterprise storage line

Providing simultaneous iSCSI and fiber channel protocol, the N3300 series is designed to address your concerns with data management in a "scale out" data center, backup & restore, and data protection disaster recovery.

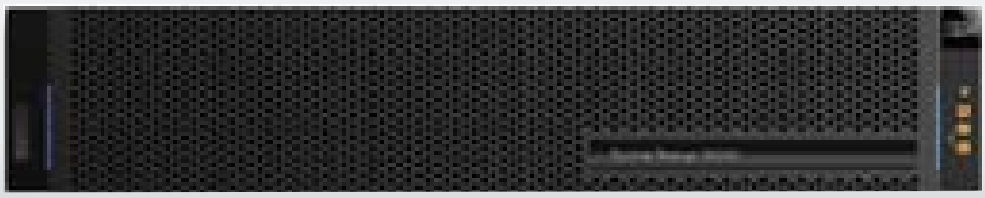
The N3300 series offers:

- >> **High availability and support**
- >> **Rapid backup and rapid recovery**
- >> **Simple replication and disaster recovery**
- >> **Management simplicity**
- >> **Versatility**
- >> **Flexibility**

Easy to administer and deploy, it can help lower overall costs and provide enterprise-class data protection in a cost-effective package.

The N3300 Series, a winning unified storage solution.

Let Softchoice build a configuration that fits your needs and budget.



IBM Business Partner

Tutorial: Network Access Control (NAC)

By Mike Fratto
Network Computing

No network is airtight—malware continues to get in, whether via mobile employees, guest or contractor laptops, or end users downloading dodgy content. Antivirus software at the gateway or on the desktop helps with computers under your control, but guests and unmanaged servers remain problematic. And let's face it: Sometimes attackers are just smarter than we are. Even companies following best practices get hit.

We don't just mean just security best practices, either. Protecting the network from malicious hosts is, ultimately, a desktop management function. NAC is what puts teeth in your policies, providing an enforcement mechanism that helps ensure computers are properly configured. By weighing such factors as whether a user is logged in; her computer's patch level; and if anti-malware or desktop firewall software is installed, running and current, IT can decide whether to limit access to network resources based on condition. A host that doesn't comply with your defined policy could be directed to remediation servers, or put on a guest VLAN.

Remember Slammer? If a company could have determined that a host was running an unpatched version of MSDE 2000 and denied access until it was patched, Slammer would have had a much less dramatic effect.

That's the promise, but NAC is no magic bullet. The solution to the Slammer scenario is to either patch the vulnerable system when you can, or remove access to MSDE from the network. But if your NAC system doesn't check for applications like MSDE or their patch levels, it wouldn't preclude a vulnerable node from accessing the network.

General Architecture

Three basic components are found in all NAC products: the Access Requestor (AR), the Policy Decision Point (PDP) and the Policy Enforcement Point (PEP); see NAC Framework diagram on adjacent page. Vendors have their own names for these, but we'll use the terms defined by the Trusted Computing Group Trusted Network Connect working group because they're fairly clear-cut.

Framework Summary

	Cisco Network Access Control	Microsoft's Network Admission Protection	Trusted Computing Group, Trusted Network Connect
Host Assessment	The Cisco Trust Agent will be used for Windows pre-Longhorn and Vista, and Red Hat Enterprise 3 and 4.	Microsoft's NAP agent and 802.1X supplicant are part of Windows Longhorn and Vista. APIs are available for other vendors to create and integrate system health agents (SHAs) into the NAP framework. The vendor is responsible for how and what the SHA communicates to the NAP client. For example, self-assessment and real-time change notification are not required.	The TNC specifications deal with communication between an AR and a PDP as well as how software can communicate with the TNC AR. Another system performs the assessment.
Validation	Credentials and assessment data are sent to the ACS for validation. The ACS sends them along to Microsoft's Network Policy Server. The ACS selects a policy based on the response from the NPS.	The NPS integrates with external Policy Servers, such as AV and patch management systems, to assess a host's health.	TNC-developed protocols and API specify how components communicate.
Enforcement	Cisco hardware is responsible for enforcing the access policy sent by the Access Control Server.	Quarantine may be accomplished by allowing or denying a host access to a VPN or integrating with external systems.	TNC-developed protocols and API specify how components communicate.
Partner Programs	Cisco has a large partner program populated with a number of well-known product vendors. Cisco and Microsoft both claim that they will be supporting their own partner programs as well as the NAC/NAP program. Microsoft is planning on migrating its partners to the new API for Longhorn and Vista.	Microsoft has a large partner program, and unlike Cisco, also has a number of infrastructure vendors in the fold. Microsoft also appears to be a strong partner with the Trusted Network Connect working group as well as with Cisco.	The specifications are available for download. Members of the TCG can participate in the working group. Microsoft has released its Statement of Health protocol for the TNC specification.
Interoperability Testing	Cisco uses AppLabs, which acquired KeyLabs, for interoperability testing in the NAC program. NAC partners are expected to develop and test their products.	Microsoft has no plans for an interoperability testing program.	The TNC is planning future compliance programs, but is otherwise mum on the issue.

Individual functions of the PDP and the PEP may be contained on one server or spread across multiple servers, depending on vendor implementation, but in general, the AR requests access, the PDP assigns a policy, and the PEP enforces the policy.

The AR is the node that is attempting to access the network and may be any device that is managed by the NAC system, including workstations, servers, printers, cameras and other IP-enabled devices. The AR may perform its own host assessment, or some other system may evaluate the host. In either case, the AR's assessment is sent to the PDP. The PDP is the brains of the operation. Based on the AR's posture and a company's defined policy, the PDP determines what access should be granted. In many cases, the NAC product management system may function as the PDP. The PDP often relies on back-end systems, including antivirus, patch management or a user directory, to help determine the host's condition. For example, an AV manager would determine whether a host's AV software and signature versions are current, and inform the PDP.

Once the PDP determines which policy to apply, it communicates the access control decision to the PEP for enforcement. The PEP could be a network device, like a switch, firewall or router; an out-of-band device that manages DHCP or ARP; or an agent on the AR itself.

NAC Cycle

When a host attempts to connect to a NAC-enabled network, there are typically three phases: pre-admission or post-admission assessment, policy selection, and policy enforcement. The criteria governing each step are based on your company's policy and your NAC system's capabilities.

Before you select a product, determine exactly what your company's goals are. For example, How far out-of-date can patches or AV signatures be before a host can no longer access the network? What is the acceptable condition for a guest host before it can have access? Do you want to base access on user ID or not?

Assessment

The NAC cycle begins and ends with assessment. Pre-admission assessment occurs before a host is granted full access to the network. Post-admission assessment, after access has been granted, enables a host to be periodically reassessed to ensure it does not begin to pose a threat. Host assessment gathers information, like a host's OS, patch levels, applications running or installed, security posture, system configuration, user login, and more, and passes it to a PDP. What information is gathered is a function of your defined policy and the NAC product's capabilities.

Copyright © 2007 CMP Media LLC.

Read the full article at **www.softchoice.com/fratto**

Shields Up Mr. CIO

(Just Make Sure They're Encrypted)

By Patrick McGregor
Optimize

I would bet that TJX executives haven't slept much lately. After watching the shock waves reverberate out from recent information security breaches, CIOs and IT managers from other companies shouldn't be getting any sleep either.

Enterprises from retail and other industries must implement fundamental changes to their approach to information security. Unless you have been hiding in a bunker, you've heard about the massive cardholder data breach at TJX. TJX, the parent company of Marshall's and T.J. Maxx, recently revealed that hackers penetrated its computer systems and obtained sensitive information associated with 45 million credit card and debit card accounts.

This egregious incident will likely cost TJX millions of dollars in investigation fees, legal settlements, and consumer protection programs. In addition to the $5 million in costs that TJX has already incurred in connection with this incident, currently TJX is facing:

- A class-action lawsuit filed on the behalf of 300 banks that claims tens of millions of dollars in damages.
- Investigations from attorneys general from 30 states.
- Investigations from the FTC and Canadian privacy organizations.
- Twenty other lawsuits filed by TJX consumers and shareholders.

The TJX breach is the largest ever publicly reported, but it is certainly not the first. Hundreds of organizations have disclosed serious breaches during the past few years, including:

- In 2005, intruders stole over 40 million credit card account numbers by hacking into CardSystems Solutions' computer systems, resulting in millions of dollars in fraudulent purchases. This breach led the company to file for bankruptcy.
- In the same year, data thieves hacked into a DSW Shoes database. The intruders obtained 1.4 million credit card numbers and names associated with those accounts, as well as other information, such as driver's license and checking account numbers.
- In 2006, a thief stole an unencrypted laptop belonging to an agent at the U.S. Department of Transportation Law enforcement has yet to recover the laptop, which contained over 130,000 social security numbers. This incident is one of many recent data breaches reported by the federal government.

Despite these high-profile incidents, intrusions and thefts continue to occur. According to the Privacy Rights Clearinghouse, dozens of organizations have revealed breaches since the 2007 TJX announcement, including the IRS, the California National Guard, and Speedmark.

Why are these breaches growing in number and in degree of damage? The answer is simple: Most companies are just not protecting sensitive data from the moment of creation to the moment of deletion. In today's IT environments, achieving data security is a daunting task, and many enterprises do not invest in resources that are critical to addressing key security problems.

Retailers Are Particularly Targeted

Retail companies, in particular, are attractive hacking targets for several reasons. For instance, it is easier to capitalize on a retail security breach than it is to profit from thieving information from other classes of companies. Upon stealing intellectual property from a manufacturing company or patient data from a health care provider, a culpable hacker needs to find a buyer to profit from the security breach. In contrast, a hacker that surreptitiously obtains cardholder data from a retail company is stealing virtual money: Criminals can immediately utilize the compromised cardholder information to acquire assets or generate cash.

Another reason for retailers being targeted involves the exposure of their IT systems to the public. Retail information technology systems are more accessible to potential intruders than that of other industries due to the distribution and physical organization of retail stores. As opposed to a law firm or a financial services company that may employ physical security controls to separate customers from systems that process sensitive data, retail customers have direct access to systems that contain cardholder information. In retail environments, an intruder may find opportunities to physically steal cash registers, sniff Internet transmissions to back-end processing centers, or exploit wireless networks to attack in-store IT systems. Hope exists, however. Retail and other enterprises can " and must " capitalize on tools and resources that are available today. Enterprises can prevent breaches similar to those experienced by TJX and DSW by implementing proactive corporate processes, procuring next-generation information security technologies, and frequently assessing the state of their systems' security against known threats. Of course, this will require investments of time and cash. When considering the probable devastating result of not taking action, however, the correct choice is clear.

Copyright © 2007 CMP Media LLC.

Read the full article at
www.softchoice.com/mcgregor

The Next Generation of Symantec AntiVirus

New Symantec Endpoint Protection 11.0

Symantec™ Endpoint Protection combines Symantec AntiVirus™ with advanced threat prevention to deliver an unmatched defense against malware such as viruses, worms, spyware, Trojan horses, zero-day threats, and rootkits. This unified product delivers the most advanced technology available to protect against today's sophisticated threats and threats not seen before. It increases protection for laptops, desktops, and servers by including proactive technologies that automatically analyze application behaviors and network communications to detect and actively block threats. It is a single, comprehensive product that allows you to enable the capabilities you need as you need them. Whether the attack comes from a malicious insider or is externally motivated, endpoints are protected.

This multilayered approach significantly lowers risk and increases confidence that business assets are protected. Symantec Endpoint Protection reduces the administrative overhead and costs associated with managing multiple endpoint security products by integrating essential security technologies in a single agent that is administered via a single management console. This simplifies endpoint security administration and provides operational efficiencies such as one-click software updates and policy updates, unified and central reporting, and a single licensing and maintenance program.

symantec™

www.softchoice.com/symantec

WANTED
VIRUS-INFESTED PCs

Your network may not be as secure as you think...
We can help you spot the troublemakers.

Roughly 49% of all business PCs contain moderate to severe spyware infestations, while one in every 16 is likely missing anti-virus software altogether.* Good thing we offer the Softchoice TechCheck™. By leveraging data from any type of IT management solution, a Softchoice TechCheck can help you spot missing patches, service packs, and anti-virus software and a whole lot more. The best part? You can dramatically reduce your security risks with almost no time or resources invested on your part. Now that's peace of mind!

Take the guesswork out of your network.
Call 1.888.SOFTCHOICE or visit www.softchoice.com/techcheck

softchoice
Tech Check™

**Unnecessary Expenditures, Unnecessary Risks: Trends and Opportunities in IT Policy Management.* Softchoice Corporation, June 2006.